Sujet élaboré par une cellule pédagogique nationale

EXAMEN PROFESSIONNEL D'AVANCEMENT DE GRADE DE TECHNICIEN PRINCIPAL TERRITORIAL DE 1ère CLASSE

SESSION 2019

ÉPREUVE DE RAPPORT AVEC PROPOSITIONS OPÉRATIONNELLES

Rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt. Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGÉNIERIE, INFORMATIQUE ET SYSTÈMES D'INFORMATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 28 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.

S'il est incomplet, en avertir le surveillant.

Vous êtes technicien principal territorial de 1ère classe, en qualité de délégué à la protection des données, au sein de la direction des systèmes d'information de la communauté d'Agglomération de Techniagglo (65 000 habitants).

Dans un premier temps, le directeur des systèmes d'information vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur le règlement général sur la protection des données (RGPD).

10 points

Dans un deuxième temps, il vous demande d'établir un ensemble de propositions opérationnelles visant à mettre en conformité le système d'information de la communauté d'agglomération avec la nouvelle réglementation.

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances

10 points

Liste des documents :

Document 1 « RGPD : cinq façons de respecter vos obligations de sécurité ».
Martien Ouwens - blogs.oracle.com - Juin 2018 - 3 pages.

Document 2 « Evaluer le niveau de sécurité des données personnelles de votre organisme - La sécurité des données personnelles » *(Extrait).*
C.N.I.L. - Les guides de la C.N.I.L.- Edition 2018 - 2 pages.

Document 3 « Comment assurer la protection de vos données personnelles ».
infodsi.com - Octobre 2018 - 4 pages.

Document 4 « Comment sécuriser son réseau interne après le RGPD ? ».
Marilyne Michel - journaldunet.com - Juin 2018 - 1 page.

Document 5 « Repenser la sauvegarde des données à l'heure du RGPD ».
Hervé Collard - journaldunet.com - Juin 2018 - 3 pages.

Document 6 « Quel rôle pour le RSSI et le DPO ? ».
informatiquenews.fr - Mai 2018 - 2 pages.

Document 7 « RGPD : la mutualisation des SI des collectivités en vue ».
Frédéric Charles - zdnet.fr - Juin 2018 - 3 pages.

Document 8 « Règlement général sur la protection des données » *(Extrait).*
C.N.I.L., Règlement (UE) 2016/679 du Parlement européen et du Conseil 17/04/2016 - Mai 2018 - 1 page.

Document 9 « Recommandations relatives à l'administration sécurisée des systèmes d'information » *(Extrait).*
Agence nationale de la sécurité des systèmes d'information - Avril 2018 - 4 pages.

Document 10 « La mise en œuvre du RGPD dédramatisée au Congrès des maires ».
Gabriel ZIGNANI - Lagazettedescommunes.fr - Novembre 2018 - 2 pages.

Certains documents peuvent comporter des renvois à des notes ou à des documents non fournis car non indispensables à la compréhension du sujet.

DOCUMENT 1

« RGPD : cinq façons de respecter vos obligations de sécurité ».

Martien Ouwens - blogs.oracle.com - Juin 2018.

Le RGPD est désormais en vigueur. Êtes-vous totalement en règle ? Voici, selon nous, les cinq grandes priorités qui vous permettront de prouver le respect de vos obligations de sécurité des données.

Après plus de deux ans d'attente, le Règlement général sur la protection des données (RGPD) est entré en vigueur le 25 mai dernier. Ce nouveau texte de loi européen a pour vocation d'homogénéiser et de renforcer la protection des données personnelles lors de leur traitement.

Si les amendes que risquent les entreprises contrevenantes ne vous auront certainement pas échappé, sachez que le règlement va plus loin. Des interdictions potentielles de traitement de données aux droits des personnes concernées, en passant par les indemnisations en cas de violation de sécurité, vous avez tout intérêt à bien peser chacune de vos décisions de mise en conformité.

Par conséquent, vous vous êtes peut-être déjà penché sur des questions essentielles comme la gestion des consentements, les tâches de découverte de données clés et le respect des droits d'accès, de rectification, à la portabilité et à l'oubli des personnes concernées. Toutefois, quel que soit l'état d'avancement de votre mise en conformité au RGPD, vous devez aussi explorer les dernières technologies de sécurité et de protection des données. C'est ce qu'énonce implicitement la règlementation dans son article 32 (sécurité des traitements). En effet, elle y exige que les responsables de traitement et leurs sous-traitants implémentent des mesures techniques appropriées afin de garantir en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et des services de traitement.

Les conditions étant posées, vous trouverez ci-dessous les cinq grandes priorités pour bien réussir votre mise en conformité.

1. **Veillez à pouvoir démontrer votre respect du principe de responsabilité**

   À partir du mois de mai, la transparence de vos traitements de données revêt une importance plus capitale que jamais. En effet, votre capacité à justifier de vos modes de gestion des données et des mesures prises pour assurer la sécurité des traitements (afin de garantir la confidentialité, l'intégrité et la disponibilité des données) constitue un élément clé de votre conformité au RGPD.

   Pour satisfaire au principe de responsabilité, vous devez également documenter vos décisions technologiques. En d'autres termes, vous devez notamment pouvoir expliquer la logique d'investissement dans telle ou telle technologie destinée à réduire les risques d'intrusion ou faciliter vos investigations à la suite d'une violation de données.

2. **Envisagez des fonctionnalités de chiffrement et de pseudonymisation**

   Il est vrai que les technologies conçues pour favoriser votre mise en conformité au RGPD sont légions. Toutefois, la règlementation ne vous *oblige* explicitement à rien : il vous revient de prendre vos propres décisions, en tenant compte des technologies disponibles, des coûts d'implémentation et de la nature, de la portée, du contexte et des finalités de votre traitement de données – sans oublier les droits des personnes concernées.

   Ceci étant dit, les fonctionnalités mentionnées dans le RGPD n'y figurent pas par hasard. Elles constituent des exemples d'outils puissants qu'il est conseillé d'envisager. Par exemple, les articles 32 et 34 citent les technologies de chiffrement et de pseudonymisation. Vous aurez donc tout intérêt à examiner ces technologies et à déterminer leurs avantages pour vous et les personnes concernées dont vous détenez

les données. À titre d'exemple, le chiffrement et le masquage de base de données offrent des moyens simples de chiffrer et de pseudonymiser les données. En prime, leur déploiement et leur implémentation s'avèrent relativement faciles.

3. **Mettez en place des contrôles d'accès adaptés**

   Sans l'implémentation de politiques et mesures adaptées de contrôle des accès, même la meilleure solution de protection des données ne vaudra pas grand-chose.

   D'où l'importance de paramétrer les fonctionnalités suivantes :

   - **Autorisation** : déterminez qui peut accéder à quelles données. Pour diminuer votre surface d'attaque, réduisez les droits de chacun au strict minimum nécessaire pour exécuter les tâches qui lui incombent. De même, établissez des politiques destinées à prévenir les erreurs et les contournements.
   - **Authentification** : veillez à ce que vos systèmes puissent vérifier l'identité de la personne, du compte, de l'objet, du système ou de la procédure demandant l'accès.

   En mettant en place des contrôles adaptés, vous pourrez opérer en toute sérénité. En cas de problème, vous pourrez facilement et rapidement remonter à la source pour prouver votre bonne foi et fournir des d'informations détaillées sur les éventuelles fuites.

4. **Analysez régulièrement vos logs et stockez-les de façon responsable**

   Les logs jouent un rôle essentiel dans la prévention des violations de données et, en cas d'incident, dans l'enquête sur les responsabilités des différentes personnes ou systèmes responsables.

   Ils vous aideront sur plusieurs tableaux :

   - Analyse et prévention des incidents
   - Compréhension des événements pour éviter toute récidive
   - Reconstitution des événements et des causes sous-jacentes

   Même dans le pire des scénarios, les logs fourniront la preuve de votre conformité, ce qui réduira les sanctions à votre encontre.
   Ces logs et pistes d'audit devront couvrir l'ensemble de vos ressources IT (applications, bases de données, pare-feu, middleware, etc.) tant sur site que dans le cloud.

5. **Maintenez vos systèmes à jour à l'aide de correctifs et d'une configuration sécurisée**

   Le plus souvent, les violations de données sont imputables à des logiciels obsolètes, non corrigés. Quand on sait que l'application de correctifs peut entraîner des interruptions de service, on s'étonne beaucoup moins du retard de nombreuses entreprises dans leurs opérations de mise à jour.

   Toutefois, les nouveaux systèmes facilitent grandement ce processus. Par exemple, les logiciels et outils de découverte et de gestion des correctifs aident les entreprises à maintenir la disponibilité des systèmes et des données personnelles qu'ils hébergent.

Pour approfondir la question

Il est important de bien comprendre que le RGPD ne vise pas à sanctionner les entreprises non conformes. Sa vraie vocation est de renforcer la sécurité des données des personnes physiques.

Certes, les cinq priorités ci-dessus vous aideront à prendre des mesures essentielles pour votre mise en conformité au RGPD. Mais, au final, le Règlement vise avant tout à instaurer de bonnes pratiques de gestion de la sécurité des données et à rapprocher les personnes physiques des dépositaires de leurs informations.

Pour rester en règle sur le long terme, vous devrez sans cesse moderniser vos systèmes de sécurité. Misez sur les dernières avancées technologiques pour améliorer et optimiser en continu vos modes de protection des données.

DOCUMENT 2

« Evaluer le niveau de sécurité des données personnelles de votre organisme - La sécurité des données personnelles » *(Extrait).*
C.N.I.L. - Les guides de la C.N.I.L. - Edition 2018.

ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE VOTRE ORGANISME

Avez-vous pensé à ?

	FICHES	MESURE	
1	Sensibiliser les utilisateurs	Informez et sensibilisez les personnes manipulant les données	☐
		Rédigez une charte informatique et donnez lui une force contraignante	☐
2	Authentifier les utilisateurs	Définissez un identifiant (login) unique à chaque utilisateur	☐
		Adoptez une politique de mot de passe utilisateur conforme à nos recommandations	☐
		Obligez l'utilisateur à changer son mot de passe après réinitialisation	☐
		Limitez le nombre de tentatives d'accès à un compte	☐
3	Gérer les habilitations	Définissez des profils d'habilitation	☐
		Supprimez les permissions d'accès obsolètes	☐
		Réaliser une revue annuelle des habilitations	☐
4	Tracer les accès et gérer les incidents	Prévoyez un système de journalisation	☐
		Informez les utilisateurs de la mise en place du système de journalisation	☐
		Protégez les équipements de journalisation et les informations journalisées	☐
		Prévoyez les procédures pour les notifications de violation de données à caractère personnel	☐
5	Sécuriser les postes de travail	Prévoyez une procédure de verrouillage automatique de session	☐
		Utilisez des antivirus régulièrement mis à jour	☐
		Installez un « pare-feu » (*firewall*) logiciel	☐
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	☐
6	Sécuriser l'informatique mobile	Prévoyez des moyens de chiffrement des équipements mobiles	☐
		Faites des sauvegardes ou des synchronisations régulières des données	☐
		Exigez un secret pour le déverrouillage des smartphones	☐
7	Protéger le réseau informatique interne	Limitez les flux réseau au strict nécessaire	☐
		Sécurisez les accès distants des appareils informatiques nomades par VPN	☐
		Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi	☐
8	Sécuriser les serveurs	Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées	☐
		Installez sans délai les mises à jour critiques	☐
		Assurez une disponibilité des données	☐

ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE VOTRE ORGANISME

FICHES		MESURE	
9	Sécuriser les sites web	Utilisez le protocole TLS et vérifiez sa mise en œuvre	☐
		Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url	☐
		Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu	☐
		Mettez un bandeau de consentement pour les *cookies* non nécessaires au service	☐
10	Sauvegarder et prévoir la continuité d'activité	Effectuez des sauvegardes régulières	☐
		Stockez les supports de sauvegarde dans un endroit sûr	☐
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	☐
		Prévoyez et testez régulièrement la continuité d'activité	☐
11	Archiver de manière sécurisée	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	☐
		Détruisez les archives obsolètes de manière sécurisée	☐
12	Encadrer la maintenance et la destruction des données	Enregistrez les interventions de maintenance dans une main courante	☐
		Encadrez par un responsable de l'organisme les interventions par des tiers	☐
		Effacez les données de tout matériel avant sa mise au rebut	☐
13	Gérer la sous-traitance	Prévoyez une clause spécifique dans les contrats des sous-traitants	☐
		Prévoyez les conditions de restitution et de destruction des données	☐
		Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)	☐
14	Sécuriser les échanges avec d'autres organismes	Chiffrez les données avant leur envoi	☐
		Assurez-vous qu'il s'agit du bon destinataire	☐
		Transmettez le secret lors d'un envoi distinct et via un canal différent	☐
15	Protéger les locaux	Restreignez les accès aux locaux au moyen de portes verrouillées	☐
		Installez des alarmes anti-intrusion et vérifiez-les périodiquement	☐
16	Encadrer les développements informatiques	Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux	☐
		Évitez les zones de commentaires ou encadrez-les strictement	☐
		Testez sur des données fictives ou anonymisées	☐
17	Utiliser des fonctions cryptographiques	Utilisez des algorithmes, des logiciels et des bibliothèques reconnues	☐
		Conservez les secrets et les clés cryptographiques de manière sécurisée	☐

DOCUMENT 3

« Comment assurer la protection de vos données personnelles ».

infodsi.com - Octobre 2018.

Que vous travailliez au siège social d'une entreprise, dans un hôpital, une université, une collectivité locale, voire un magasin ou un restaurant, ou même de chez vous, la sécurité de votre organisation est l'affaire de tous. Cependant, compte tenu du dynamisme de la mobilité, l'utilisation d'équipements personnels gagne du terrain dans le cadre professionnel…Et il en est de même des risques qui pèsent sur la sécurité du réseau. Tel est le constat dressé par Anthony Giandomenico, chercheur et Senior Security Strategist, FortiGuard Labs, qui nous donne quelques conseils judicieux :

Dans le monde, 20% des collaborateurs travaillent partiellement ou totalement de leur domicile. Une mobilité flexible et transparente au sein des entreprises devient une priorité pour assurer de réels avantages concurrentiels, ainsi qu'une demande croissante des employés. Si cette tendance invite les collaborateurs à se libérer du traditionnel fil à la patte, elle n'est pas sans faire émerger de nouveaux risques de sécurité.

Les exigences en matière de mobilité et de transformation numérique rendent les réseaux d'entreprise plus ouverts et accessibles. Et pourtant, de leur côté, les cyberattaques sont plus fréquentes et sophistiquées. Au final, les collaborateurs sont susceptibles d'entraîner fortuitement des dommages à leur entreprise, tirant parti d'une surface d'attaque étendue.

En effet, la faible sensibilisation vis-à-vis de la cyber sécurité est susceptible de vulnérabiliser un réseau compte tenu d'un dispositif ou d'une connexion à distance piraté.

Pour maîtriser les risques liés notamment à la convergence numérique des univers professionnels et personnels, les entreprises doivent promouvoir les meilleures pratiques en matière de cyber sécurité. C'est à ce titre que les fuites de données et les risques de non-conformité peuvent être jugulés, tout en assurant la flexibilité et la productivité que les collaborateurs et entreprises appellent de leurs vœux.

Favoriser une culture de la cyber sécurité

Puisque nous utilisons nos dispositifs personnels pour se connecter à distance au réseau corporate, nous sommes tous responsables de la sécurité de celui-ci.

Voici quelques pratiques que chacun d'entre nous peut adopter pour garantir une cyber sécurité de premier rang.

- **Utiliser des points d'accès sécurisés et créer un réseau dédié aux activités professionnelles**

Une bonne pratique en matière d'accès à distance au réseau consiste à utiliser un point d'accès sécurisé. Pour maîtriser les risques lors d'une connexion au réseau de votre entreprise via un hots pot Wi-Fi, il s'agit d'utiliser un réseau privé virtuel (VPN). Un VPN vous permet d'étendre votre réseau privé vers le Wi-Fi public à l'aide d'une connexion virtuelle de point à point qui sécurise les accès aux ressources corporate. Cependant, il est essentiel de se rappeler que si l'une ou l'autre extrémité de ce VPN est compromise, ce dernier n'empêchera pas des attaques du type man-in-the-middle par exemple. C'est pourquoi il est également impératif de s'assurer l'intégrité de tout point d'accès auquel vous vous connectez. Bien que les connexions Wi-Fi publiques soient souvent sans danger, il suffit d'une seule connexion malveillante pour qu'un cybercriminel intercepte toutes vos données de navigation lorsque vous passez d'un site et d'un compte à un autre.

Une autre bonne pratique à adopter consiste à créer un réseau sécurisé pour les transactions professionnelles faites de chez soi. La majorité des entreprises dispose de deux réseaux distincts, un pour les collaborateurs et l'autre pour les invités. Cette approche peut être répliquée à la maison.

En effet, les routeurs résidentiels permettent souvent d'activer de multiples réseaux (un réseau résidentiel et un réseau pour invités). En activant une protection par mot de passe pour le réseau dédié à l'activité professionnelle, vous vous assurez que vos ressources corporate n'utiliseront pas le même SSID que celui de votre console de jeu, de votre PC portable personnel ou des dispositifs de vos enfants. En dissociant vos dispositifs résidentiels du réseau utilisé pour accéder à vos données corporate sensibles, les dispositifs et applications vulnérables ne serviront pas de passerelle d'intrusion vers votre réseau d'entreprise.

- **Assurer des mises à jour régulières**

La mise à jour régulière des dispositifs, des applications et des systèmes d'exploitation est le fer de lance d'une sécurité efficace. Il est souvent tentant d'ignorer et de remettre à plus tard une mise à jour, surtout si vous travaillez sur un projet dont les délais sont sérrés ou que vous êtes en clientèle. Cependant, cette procrastination est une bénédiction pour un cybercriminel qui souhaite s'en prendre à vos dispositifs. L'un des moyens les plus efficaces et les plus faciles d'éviter cela est d'appliquer simplement des correctifs et des mises à jour, et de planifier ces actions dans votre journée.

L'application régulière des mises à jour et des patchs protège les systèmes d'exploitation et applications contre les vulnérabilités connues. L'attaqueWannaCry, qui a tiré parti de vulnérabilités Microsoft pour injecter un ransomware, souligne à quel point les mises à jour sont essentielles. Les entreprises des utilisateurs victimes de cette exaction s'en seraient sans doute sorties beaucoup mieux si elles avaient appliqué les mises à jour et patchs appropriés.

Dans le même esprit, il s'agit de s'assurer que tous les programmes et applications actifs sur un réseau d'entreprises bénéficient d'un support de la part de leurs éditeurs respectifs, et que les éléments obsolètes sont supprimés ou remplacés.

- **Une gestion des accès robuste**

La gestion des accès est une pratique simple mais ô combien efficace. D'où l'intérêt de mots de passe forts et d'une authentification à deux facteurs pour l'ensemble des dispositifs et comptes.

Les mots de passe doivent être complexes, associant caractères alphanumériques et spéciaux. Ils doivent être différents d'un compte à un autre, notamment sur les dispositifs et applications utilisés pour accéder à des données métiers confidentielles. En effet, en cas de piratage d'un compte ou d'un site et de fuite de données, les identifiants peuvent être réutilisés, via une attaque par force brute par exemple, pour pirater d'autres comptes.

Le plus grand défi pour ce type de mots de passe est simplement de s'en souvenir. La plupart des mots de passe considérés comme forts sont en fait les plus faciles à deviner. A la place, l'utilisation d'abréviation ou de phrases permet de ne pas les oublier. Par ailleurs, alors que le nombre de mots de passe dont on doit se souvenir augmente, vous pouvez également faire confiance à un gestionnaire de mots de passe pour les retrouver rapidement.

Les mots de passe associés à une authentification à deux facteurs constituent une solution encore plus intéressante. Dans ce cas, seules les personnes légitimes accèdent aux systèmes critiques et aux données sensibles. Les progrès récents de la biométrie, tels que les scanners d'empreintes digitales et les logiciels de reconnaissance faciale, permettent une authentification multifactorielle similaire. D'autre part, vous pouvez utiliser la segmentation, le contrôle d'accès au réseau et les contrôles d'accès basés sur les rôles pour limiter les utilisateurs et les dispositifs qui peuvent accéder à des informations sensibles et de grande valeur.

- **Utiliser l’email avec précaution**

L’email est le vecteur d’attaque le plus utilisé par les cybercriminels aujourd’hui. En raison de son utilisation unique, il reste le moyen le plus simple de diffuser des logiciels malveillants à des utilisateurs qui ne se doutent de rien.

Les cybercriminels tirent parti de l’email de différentes façons. Mais, au final, ils cherchent avant tout à piéger les destinataires, souvent en usurpant l’identité d’un de leurs collègues ou de leurs proches, pour les inciter à cliquer sur des liens ou fichiers joints malveillants.

Le phishing et le spear phishing comptent parmi les arnaques les plus courantes par email.

Les attaques de phishing intègrent des liens vers des sites web qui paraissent légitimes – tels que les banques, entreprises et autres organismes gouvernementaux – et qui demandent aux utilisateurs de s’y connecter, pour détourner les identifiants ou infecter le dispositif connecté à l’aide d’un malware. Le spear phishing tente de rendre ces attaques plus efficaces en usurpant l’identité d’un collègue ou d’un utilisateur de confiance, pour ensuite demander des identifiants de connexion, des données confidentielles de collaborateurs, l’exécution d’un transfert bancaire ou simplement d’ouvrir un fichier joint vérolé ou de cliquer sur un lien malveillant.

Pour juguler de telles menaces, vous devez être vigilants lorsque vous répondez aux emails, surtout ceux qui contiennent des liens ou de fichiers joints. Ne cliquez jamais sur un lien ou pièce jointe provenant d’un expéditeur inconnu. Et même si un email vous semble provenir d’une source de confiance, vérifiez néanmoins l’adresse email ou le site web vers lequel il vous dirige.

Il n’est pas rare que les noms et les URLs comportent des fautes d’orthographe, ce qui est susceptible de révéler une attaque. Même si tout semble normal, arrêtez-vous et demandez-vous si cela ressemble à quelque chose que cette personne vous enverrait ou vous demanderait de faire. La plupart du temps, les liens ne sont fournis qu'après une demande soit faite, ou dans le cadre d'une conversation plus ou moins longue. Les demandes inattendues sont TOUJOURS suspectes et peuvent justifier de contacter directement l'expéditeur non seulement pour vérifier la demande, mais aussi, s'il est légitime, pour lui suggérer d'utiliser un processus différent de la distribution de pièces jointes et de liens non annoncés.

- **Installer un anti-malware**

Si les anti-malware ne peuvent stopper les attaques inconnues, la majorité des attaques et des exploits réutilisent des exactions ayant déjà réussi auparavant. L’installation d’un anti-malware/anti-virus sur l’ensemble de vos dispositifs et réseaux offre une protection face à une attaque de phishing réussie ou une tentative d’exploiter une vulnérabilité connue. Recherchez également des outils qui offrent des fonctionnalités de sandboxing, que ce soit dans le cadre d'un package de sécurité installé ou d'un service cloud, pour détecter également les menaces Zéro-Day et autres menaces inconnues.

- **Élaborer un plan de prise en charge et de restauration des incidents**

Toutes les entreprises, quelle que soit leur taille, doivent disposer d’un plan de prise en charge et de restauration des incidents pour accélérer la reprise. Assurez-vous que tous les collaborateurs connaissent ce plan pour qu’il n’y ait pas d’hésitation sur la démarche à suivre en cas d’attaque.

Cela comprend une ligne d'assistance téléphonique afin que les employés sachent à qui s'adresser s'ils soupçonnent qu'il y a eu atteinte à la sécurité des renseignements personnels. Vous devez également vous assurer que cette ligne d'assistance soit accessible 24h/24, 7j/7, ou qu'un numéro d'urgence soit disponible en dehors des heures de travail.

Un plan simple et une sensibilisation des équipes permettront à votre entreprise de stopper rapidement la propagation d'une attaque sur l'ensemble du réseau, de réduire les délais d'indisponibilité, de minimiser l'extraction des données et d'accélérer les opérations de restauration.

La cyber sécurité n'est plus l'apanage des seules équipes informatiques et autres RSSI. Lorsque les collaborateurs interagissent avec la technologie et en dépendent chaque jour, souvent depuis des sites distants, ils deviennent tous acteurs de la sécurité de l'entreprise.

Afin de garantir la sécurité et la conformité, notamment face aux tendances croissantes de la transformation numérique et de la mobilité, chaque collaborateur se doit de comprendre et d'appliquer les meilleures pratiques en matière de cyber sécurité. En connaissant les vecteurs d'attaque courants et en utilisant les conseils ci-dessus, les utilisateurs contribuent à enrayer la propagation des malwares et à assurer le bon fonctionnement de votre entreprise.

DOCUMENT 4

« Comment sécuriser son réseau interne après le RGPD ? ».

Marilyne Michel - journaldunet.com - Juin 2018.

Comment sécuriser son réseau interne après le RGPD ?

Longtemps vu comme une simple multiprise, le réseau informatique doit apporter un minimum d'administration et de supervision. Avec la mise en vigueur du RGPD, l'entité est obligée de prévenir dans les 72h en cas de violation des données personnelles, incluant notamment l'accès non autorisé à des données. C'est alors qu'il devient important de mettre en place des outils d'administration efficaces afin de sécuriser le réseau et prévenir en cas de comportement anormal ou d'accès non autorisé.

Cartographier son système d'information

Chaque entreprise ou organisation possède des données à caractère personnel dont certaines dites sensibles telles que définies par la législation. À partir de cette liste de données sensibles, il sera possible de déterminer sur quels composants du système d'information elles se localisent afin d'identifier les serveurs et les postes critiques pour l'entité. C'est à ce titre qu'ils devront faire l'objet de mesures de sécurité spécifiques pouvant porter sur la sauvegarde, la journalisation et les accès. Ainsi, il s'agit donc de créer et de maintenir à jour une cartographie simplifiée du réseau interne, notamment les interconnexions possibles avec l'extérieur. Il faut alors se demander quelles sont les vraies sources de risque et d'évaluer ces menaces : s'agit-il d'un risque matériel, logiciel ou humain ?

Définir une politique d'accès au réseau interne

La sécurité du système d'information repose sur une bonne gestion des politiques de sécurité s'appliquant à l'ensemble du parc informatique. La difficulté réside dans l'application de ces politiques. Celles-ci doivent être simples et rapides aussi bien pour les administrateurs que pour les utilisateurs. Une manière de garantir la sécurité du système d'information est d'abord de maîtriser les équipements qui s'y connectent, chacun constituant une porte d'entrée potentielle de vulnérabilité.

Pour sécuriser le système d'information, il est conseillé de le séparer physiquement. Les serveurs, les passerelles et les matériels réseaux doivent être placés dans des salles spécifiques dont l'accès est protégé et limité aux seuls administrateurs. Ces mêmes administrateurs doivent être informés régulièrement de ce qui se passe sur le réseau afin d'identifier rapidement les activités suspectes.
Mais il faudra veiller également à segmenter virtuellement le réseau informatique afin que les utilisateurs aient accès uniquement aux données et aux ressources dont ils ont besoin et éviter l'accès et la compromission des données même de façon involontaire aux personnes non autorisées.

L'entité se doit de sensibiliser l'ensemble des utilisateurs de son réseau. Par défaut, ils ont tendance à privilégier la commodité plutôt que la sécurité. Pour contrer ces sources de risque, différentes solutions, souvent simples à déployer, existent. Encore faut-il que l'entité les identifie et s'adapte à leur usage du réseau interne : l'équipement des collaborateurs est-il fourni par l'entreprise ou par les collaborateurs eux-mêmes ?

Enfin, il ne faudra pas oublier non plus l'accès au réseau des visiteurs. Si on n'est habituellement assez vigilant avec les visiteurs occasionnels, on donne plus facilement accès aux visiteurs réguliers aux ressources de l'entreprise pour des questions de commodités encore une fois.

Quelles que soient l'infrastructure et les techniques de sécurité mises en place, si les procédures d'utilisation des outils et moyens de communication ne sont pas comprises ni respectées, les sources de risque vont augmenter et mettre en péril la sécurité interne du système d'information.

DOCUMENT 5

« Repenser la sauvegarde des données à l'heure du RGPD ».

Hervé Collard - journaldunet.com - Juin 2018.

Ce règlement ambitieux et très médiatisé a pour but d'adapter la protection des données personnelles des citoyens européens aux nouvelles réalités du monde numérique. Toutes les entreprises de l'UE sont concernées ainsi que toutes les entreprises non-européennes traitant des données de citoyens de l'UE.

Le droit à l'oubli, le droit à la modification de ses données, les restrictions en matière de collecte et de stockage des données et plus généralement le respect de la vie privée des citoyens européens sont au cœur du projet du RGPD. L'UE s'est par ailleurs dotée de pouvoirs importants pour faire respecter cette réglementation.

Il existe de nombreux articles détaillant les enjeux, les contraintes et les pénalités pour tout manquement à ce règlement. Nous sommes tous concernés -des TPE aux grands comptes- en Europe mais aussi en dehors des frontières dès lors que les données personnelles sont d'origine européenne. La présente tribune n'a pas pour objet de rajouter une énième voix à ces discussions à l'approche du 25 mai 2018. Elle vise plutôt à expliquer les enjeux du RGPD vis-à-vis de la protection des données en générale et des sauvegardes en particulier.

Quelles sont les obligations RGPD en matière de sauvegarde ?

Notons que les 11 chapitres et les 99 articles du RGPD n'adressent pas explicitement le sujet de la sauvegarde. Il adresse les pratiques nécessaires pour bien traiter les données personnelles. Ce traitement inclut la collecte, la modification, l'utilisation, la confidentialité, la structuration et la conservation des données. Implicitement, nous pouvons considérer que la sauvegarde fait partie de la conservation (Article 4).

L'article 32 impose aux responsables du traitement des données (et à tous les sous-traitants) de mettre en œuvre des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».

Ces mesures incluent :

- La pseudonymisation et le chiffrement des données personnelles
- Une garantie de confidentialité, intégrité et la disponibilité des données traitées
- La possibilité de rétablir la disponibilité des données en cas d'incident
- Une évaluation des risques et un suivi des mesures de sécurité du traitement mises en place

Nous sommes ici au cœur du sujet. Voici les piliers d'une conformité et des obligations que toute solution de sauvegarde devrait respecter :

- Le chiffrement de toute donnée en transit ou en stockage -y compris dans les données sauvegardées. Les droits d'accès, de duplication et de restauration des données ainsi que les opérations effectuées doivent aussi être très contrôlés (audit trails).
- Le cloisonnement des données, qui permettra une restauration sûre et fiable d'une donnée ciblée (fichier, VM, base de données…) ou d'un Disaster Recovery complet en cas d'incident majeur.

- Un bon niveau de reporting. Une organisation qui gère des données personnelles doit savoir où se trouvent les données de ses clients. Si une violation des données (data breach) est avérée, a-t-elle impacté les données primaires ou toutes les données y compris les sauvegardes, et si oui lesquelles.

Le RGPD prévoit que tout citoyen a la possibilité d'accéder, modifier et effacer ses propres données personnelles. L'organisme qui traite ces données doit pouvoir les localiser puis les modifier, les effacer et les déplacer si besoin. Depuis un stockage primaire, ceci est typiquement assez simple. S'agissant d'une sauvegarde des données, les choses peuvent se compliquer. Est-il par exemple si simple d'effacer des tables dans une base de données qui se trouvent sur une ou plusieurs bandes LTO dans un coffre-fort ?

Accéder et modifier chaque exemple d'une donnée client sur plusieurs supports relève parfois du défi et pourrait s'avérer très coûteux. Une donnée personnelle est souvent copiée et donc multipliée au sein de plusieurs stockages et sauvegardes (locales, distantes, sur disque, sur bande, dans le Cloud…).

Au vu des contraintes et des recommandations du RGPD, une réponse pragmatique consisterait à mettre en place :

- Un recyclage des jeux de sauvegarde après un délai raisonnable (quelques semaines typiquement). La sauvegarde, oui, mais pas pour toujours ! Evitons également le data sprawl ou la prolifération souvent non-contrôlée des données.

- Un archivage plus long reste possible car certaines données doivent par nature être conservées plus longtemps. Par contre, il est essentiel de savoir où se trouve toute copie d'une donnée personnelle.

- Une pseudonymisation des informations personnelles qui réduit les risques de fuites ou d'exploitation non autorisée. Gommer les informations permettra de ne plus identifier des individus dans un fichier ou une base. Bien entendu, la pseudonymisation s'effectue en amont de toute phase de sauvegarde.

La certification RGPD n'existe pas encore. Mais il abonde de bonnes pratiques. Parmi ces pratiques, il y a une maîtrise de toute la chaîne de sauvegarde via une solution centralisée et unique ce qui permet d'assurer aussi bien la protection des données sur les postes de travail que dans les data centers. Autre dimension, la capacité à rechercher des données à sauvegarder dans les fichiers non-structurés.

Vers une protection des données conforme

Que vos données clients soient non-structurées (fichiers, images, emails etc.) ou structurées (bases de données) ou un mélange, le RGPD impose que votre infrastructure de protection et de stockage possède :

- Un contrôle centralisé et un niveau d'automatisation intégrés dans la solution de sauvegarde. Il doit être possible de choisir par inclusion ou exclusion les données à protéger et les rétentions qui s'imposent quel que soit le support de stockage.

- Un catalogue centralisé qui trace toutes les actions de sauvegarde et d'archivage avec une identification fine des objets (par nom, métadonnée, date...). Une recherche multicritère des données doit être réalisable avec une cartographie des stockages associés à chaque donnée.

- Un niveau de reporting permettant de démontrer la cohérence de la solution. Où se trouve les données, qui a effectué des restaurations, les données ont-elles bien été recyclées ?

Le RGPD nous impose une vraie réflexion et des actions concrètes sur le traitement des données personnelles. Il nous oblige à inscrire ces actions dans la durée. Si nous perdons les données de nos clients, si nous les compromettons, si nous n'arrivons pas à les localiser correctement ou si nous ne les recyclons pas au-delà de leur vie utile, nous ne serons pas en conformité face aux règlements.

Nous avons aujourd'hui de nombreux risques qui pèsent sur la donnée : cybercriminalité, erreur humaine, catastrophes naturelles… Les enjeux réglementaires formulés dans le RGPD fournissent un cadre utile nous permettant d'agir sereinement et en toute transparence.

DOCUMENT 6

« Quel rôle pour le RSSI et le DPO ? ».

informatiquenews.fr - Mai 2018.

Les RSSI (responsable de la sécurité des systèmes d'information) et les délégués à la protection des données personnelles (DPO ou Data Protection Officer), nouveau poste imposé par le RGPD ont des finalités différentes et des objectifs communs.

C'est une des idées force qui ressort de la conférence organisée récemment par le CLUSIF sur la complémentarité des RSSI et des DPO à l'approche de la date fatidique du 25 mai, correspondant à la mise en application du RGPD. Pour Thierry Chiofalo, membre du conseil d'administration du CLUSIF a *« ceux-ci visent des finalités différentes avec des objectifs communs : les premiers protègent les entreprises, les seconds les personnes. Mais les moyens et certains objectifs sont souvent communs ».*

Une démarche convergente en matière de sécurité

Les travaux du groupe de travail sur le DPO/RSSI ont montré qu'il n'existait pas de profil type de DPO mais aussi que l'on assistait à une démarche convergente en matière de sécurité. Sur le plan de la réglementation (Loi de Programmation militaire, NIS, RGPD), entre le secteur privé et le secteur public, en ce qui concerne la sécurité opérationnelle et la gestion du risque et de la conformité. *« La démarche est désormais cohérente et pluridisciplinaire entre RSSI, CIL, DPO, avocats, juristes, spécialistes techniques »*, a précisé Thierry Matusiak, membre du groupe de travail qui vient de publier deux livrables. Le premier est une infographie permettant de se préparer à la conformité attendue le 25 mai. Elle peut être téléchargée en français et en anglais sur le site du CLUSIF et a rencontré un vif succès au FIC où elle a été distribuée. Le second livrable « est une foire aux questions (FAQ) qui sera publiée au fil de l'eau, y compris après la date du 25 mai », a indiqué Dominique Soulier.

Selon le groupe de travail *« Il y a beaucoup de points communs et de synergies entre RSSI et DPO. Tant sur le plan des compétences, techniques ou juridiques par exemple, qu'en ce qui concerne leur savoir-être (vulgariser, communiquer, avoir un bon relationnel) ».*

Le RSSI et le DPO doivent travailler ensemble

Matthieu Grall, représentant la CNIL a évoqué la mise en place d'un *Privacy Impact Assessment* (PIA) : *« Le PIA est un moyen pour se mettre en conformité et de le démontrer »*. La démarche passe par une compréhension claire des traitements de données à caractère personnel et du cycle de vie des données, une identification des scénarios de risque pouvant avoir des conséquences sur les personnes concernées, et enfin la définition des mesures de sécurisation permettant de garantir la sécurité des données des personnes. *« Cette démarche permettra aussi, en cas d'incident, de mieux déterminer les répercussions sur les personnes concernées et, ainsi, les mesures d'urgence à prendre »*, poursuit Matthieu Grall. *« Le RSSI et le DPO doivent travailler ensemble et associer les métiers de l'entreprise qui sont les plus à même de décrire les traitements ».*

Cet avis est notamment partagé par Robert Eskenazy et Didier Henin, respectivement DSI et RSSI de BUT qui ont œuvré en binôme depuis trois ans pour transformer en profondeur le leader français de l'équipement de la maison. *« Il faut que les entreprises évoluent et prennent conscience que les données récoltées auprès des clients doivent être protégées »*, souligne Robert Eskenazy. BUT a dû évoluer avec l'expansion du e-commerce : partager les données entre magasins et en temps réel, utiliser des progiciels du marché. Tout en ne faisant pas table rase du passé et de l'histoire de l'entreprise.

Pour ce faire, il a fallu affiner la prise en compte de la notion client, mieux le connaître tout en prenant en compte résolument la sécurité des données collectées et leur usage.

Cela implique des actions auprès des métiers et des sous-traitants., *« Il y a un changement des mentalités à réaliser »*, considère Robert Eskenazy.

Didier Henin, pour sa part, souligne la nécessaire cartographie des traitements de toutes les données de l'entreprise, la revue des contrats, la mise en place d'exigences dès les appels d'offres, notamment en matière de sécurité des données personnelles. Mais aussi la nécessité de sonder les partenaires pour déterminer où ils se situent en matière de conformité à l'approche du 25 mai. Le RSSI de BUT a enfin estimé que le point le plus délicat était sans doute la sensibilisation du personnel.

Olivier Foret, Correspondants Informatique et Libertés (CIL) de Pages Jaunes rappelle que son groupe avait entamé une profonde mutation après un contrôle de la CNIL. Il a pris la tête d'une équipe pluridisciplinaire composée de juristes et d'un ingénieur sécurité. Il a fallu cartographier les données personnelles réparties au sein du système d'information, les catégoriser. Un RSSI a été embauché et ils travaillent désormais en binôme. Chacun se nourrit des travaux de l'autre et leur complémentarité se traduit par une meilleure information au sein de l'entreprise, y compris au plus haut niveau de management.

DOCUMENT 7

« RGPD : la mutualisation des SI des collectivités en vue ».

Frédéric Charles - zdnet.fr - Juin 2018.

Le **RGPD** qui vise à assurer un traitement adéquat des données des citoyens européens a peut-être été imaginé avec les GAFAs en tête, mais il s'applique à tous ceux qui traitent ces données personnelles.

Et il y a des acteurs auxquels on ne pense pas immédiatement et dont pourtant l'impact du RGPD sur elles sera très fort : les collectivités locales.

En France, ce sont les municipalités, conseils départementaux et régionaux et les EPCI qui sont bien sûr totalement concerné par le règlement et où **certains élus, éloignés des sujets numériques, découvrent que leur responsabilité est engagée !** Toutes les collectivités en Europe le sont également concernées.

Et oui les collectivités exploitent de nombreuses bases de données avec notamment les données personnelles de leurs administrés, vous, moi et 65 millions de français, mais également d'européens, pour les dizaines de services gérés, de la cantine scolaire de vos enfants, à l'État civil en passant par l'e-administration qui ouvre le champ de la cyber sécurité.

Contrairement aux bases de données des administrations centralisées, **ces données sont réparties dans les milliers de systèmes d'information de cette administration territoriale décentralisée sur plus de 35.000 communes.**

Ceci augmente ainsi l'effort de sécurisation et de mise en œuvre du RGPD. Ainsi les 5,8 millions de français (9%) habitent dans des villes de moins 1.000 habitants, et les 53% dans une ville de moins de 10.000 habitants, montrent de facto l'éparpillement des données personnelles sur le territoire et les redondances certaines entre tous ces SI.

Mais la tendance générale est quand même au regroupement des systèmes d'informations au niveau des intercommunalités ou des métropoles comme l'ont montré les réorganisations suite à la mise en place de la loi Notre qui met en place la réforme territoriale.

Dans ce contexte, on se demande comment l'arsenal du RGPD, à commencer par la mise en place d'un DPO (Data Privacy Officer) est possible dans toutes les communes. Le RGPD vient de monter la barre requise pour la compétence de traitement des données. Un premier impact sera certainement la poursuite accélérée d'une centralisation des systèmes d'information. Moins de SI mais plus conformes, proposés comme services (ça rappelle le développement du SaaS dans les entreprises), reste une tendance dans une économie de plus en plus numérique.
Cette semaine se tenait à la **Maison de la Chimie** à Paris une conférence sur "les collectivités territoriales faces au défi du RGPD". **GreenSI** est allé y jeter une oreille. Deux tables rondes s'y sont tenues pour répondre à la question de savoir si ce règlement était une contrainte ou une opportunité, et comment en optimiser la mise en œuvre.

Le premier enseignement de ces échanges est que l'arrivée tardive de la loi qui transpose le RGPD (arrivée cette année pour une loi européenne de 2016) et l'absence de préparation et d'accompagnement des collectivités pour la mise en conformité, sont à l'origine des **multiples interrogations, voir difficultés, au sein des petites communes et des élus. En premier lieu bien sûr la question du financement de l'adaptation des systèmes d'information.**

L'État s'est attribué un statut spécial en s'exonérant des amendes de la CNIL, mais les collectivités n'en bénéficieront pas (malgré la tentative du Sénat qui l'a proposé) et elles ne recevront pas non plus d'aides de l'État pour en supporter le coût de mise en conformité. Comme toutes les collectivités devront être conformes, même si on entend dans les couloirs que la CNIL ne va pas les viser en premier, elles vont devoir s'adapter en notamment nommer un DPO.

Une possibilité envisagée est la mutualisation des DPO. Cette mutualisation permettra le partage de compétences entre petites communes, avec ce profil issu de l'informatique, du juridique et ou du contrôle interne.

Le côté positif c'est que le règlement va demander à ces communes de se réapproprier les données qu'elles possèdent, de mieux les cartographier, d'en identifier les données personnelles, et pour certaines pourquoi pas de réfléchir à leur valorisation. Mais pour **John Billard** Vice-Président, en charge du numérique, de l'association des Maires Ruraux de France (**AMRF**), le RGPD rajoute des contraintes, notamment l'obligation de sécurisation des données, à des mairies qui ne sont ni préparées, ni accompagnées.

Faire porter le rôle de la transformation numérique dans l'équipe municipale devient donc une priorité pour sensibiliser largement.

Pour les moyens techniques, les collectivités qui passent par des prestataires du domaine privé, vont certainement pouvoir monter en compétence plus vite et exploiter la mutualisation offerte par ces entreprises.

Mais la collectivité n'est pas isolée dans ses traitements de données, et les Départements vont concentrer de nombreuses données et ainsi augmenter naturellement le risque à cet échelon

Ces échanges réguliers de données au sein du "mille-feuille" (département, agences, ...) doivent être revus pour être sécurisés, quand dans le même temps la loi pour une République numérique de 2016 a mis en avant l'obligation de l'**open data** pour les communes de plus de 3.500 habitants qui va augmenter le nombre d'échanges.

Certes, l'open data ne concerne pas les données personnelles, mais, avec la sophistication croissante des algorithmes, de plus en plus de données vont rentrer dans la catégorie des données personnelles. Il y a des points communs entre le RGPD et l'open data et même avec la Smart City, comme la démarche de recensement des données et un objectif d'aller vers une meilleure connaissance des données et de qui les utilisent. **La maîtrise des données et de leurs flux, devient donc un enjeu pour toutes les collectivités, une base pour faire reposer une nouvelle gouvernance de la donnée.**

Autre acteur avec qui la collectivité interagit : l'usager.

On assiste ici à une transformation profonde de la relation usagers avec l'avènement d'un "usager acteur", qui a des droits nouveaux vis-à-vis de ses données. Le mode de pensée précédent mettait en avant le côté irréprochable de l'administration, qui se déclinait de facto dans son système d'information, mais sans trop avoir besoin de le démontrer à l'usager. Le RGPD demande lui une déclaration à priori des traitements effectués, une acceptation par les usagers, un accès aux données et la démonstration de l'assurance à tout moment de la protection de ces données. Après tout si le RGPD est arrivé là pour donner le pouvoir à l'usager de se défendre contre les GAFA, cela fonctionne aussi avec des collectivités peu scrupuleuses dans l'usage ou la protection des données.

Pour **GreenSI** il ressort de ces débats que **le RGPD vient d'enclencher le compte à rebours de la centralisation des systèmes d'information des collectivités locales pour atteindre une conformité à un coût raisonnable.**

Les grandes collectivités et les territoires comme la Manche, qui ont déjà monté la compétence des SI en support de toutes les communes, n'ont pas attendu le RGPD pour engager cette rationalisation. **Mais les petites collectivités n'auront pas d'autre choix que de partager leur DPO et les traitements informatiques standards avec d'autres collectivités.**

C'est aussi un signal fort pour toutes les collectivités pour engager une transformation autour des données, de bénéficier de plus de transversalité en interne, de leur ouverture en open data en externe, voir jusqu'à leur valorisation avec des tiers.

Devant ces nouveaux enjeux de mutualisation, de sécurisation des données, de big data et de centralisation des traitements, le Cloud a quelques atouts. C'est donc dommage que les projets de clouds souverains engagés par l'État il a plus de 5 ans (CloudWatt, Numergy) aient échoués, car avec l'entrée en vigueur le mois dernier du "Cloud Act" qui permet à l'Administration américaine de mettre la main sur les données hors de son territoire, l'offre Cloud est réduite pour les collectivités.

GreenSI n'est donc pas surpris cette semaine par **Outscale** (racheté par Dassault Systèmes) qui annonce aux **Cloud Days**, lancer un Cloud dédié au secteur public. **La transformation numérique des collectivités locales passera d'abord par celle de leur infrastructure.**

DOCUMENT 8

« Règlement général sur la protection des données » *(Extrait).*

C.N.I.L., Règlement (UE) 2016/679 du Parlement européen et du Conseil 17/04/2016 - Mai 2018.

Règlement général sur la protection des données

CHAPITRE IV - Responsable du traitement et sous-traitant

Section 2 - Sécurité des données à caractère personnel

Article 32 - Sécurité du traitement

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

   a) la pseudonymisation et le chiffrement des données à caractère personnel;
   b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
   c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
   d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

DOCUMENT 9

« Recommandations relatives à l'administration sécurisée des systèmes d'information » *(Extrait).*

Agence nationale de la sécurité des systèmes d'information - Avril 2018.

Annexe B – Aspects juridiques

La sécurité des systèmes d'information passe par des mesures techniques mais également fonctionnelles qui intègrent des obligations pesant sur l'entité. L'administrateur est devenu un acteur clé de la sécurité des systèmes d'information sur lequel pèsent des responsabilités accrues.

Ces recommandations n'ont pas vocation à être exhaustives et nécessitent de consulter un conseil juridique spécialisé pour plus de détails.

Tout d'abord, l'administrateur est tenu à des obligations de :

- **Loyauté :** l'administrateur étant investi de larges pouvoirs de surveillance sur les données qui circulent sur les systèmes d'information de l'entreprise, le respect de règles d'éthique est attendu de sa part. Compte tenu de la « dépendance » de l'entreprise à l'égard de ce type de fonctions, la jurisprudence a tendance à se montrer plus sévère en cas de non-respect par l'administrateur de ses obligations. Des sanctions pénales peuvent être prononcées à son encontre [11], tout comme la faute grave peut être retenue dans le cadre d'une procédure de licenciement [12] ;

- **Transparence :** l'administrateur doit exercer ses missions dans le cadre du règlement intérieur et de la charte informatique édictés par l'entreprise. La charte informatique est un véritable outil de sensibilisation des salariés qui leur est opposable dès lors qu'elle est annexée au règlement intérieur. Son non-respect s'analysera en une violation du contrat de travail pouvant donner lieu à des sanctions disciplinaires, y compris un licenciement. A contrario, tolérer des agissements pourtant contraires à ce qui est prévu par la charte informatique conduira à l'absence de sanction [13] ;

- **Confidentialité :** l'administrateur est tenu à une obligation particulière de confidentialité [14], tenant notamment au secret professionnel. Il ne doit pas divulguer les informations auxquelles il aurait pu avoir accès lors de l'exercice de ses fonctions, a fortiori lorsqu'elles sont couvertes par le droit à la vie privée ou le secret des correspondances, à moins qu'une disposition législative ne l'impose (ex. en cas de découverte de contenus illicites).

Par ailleurs, l'entité doit prendre les mesures nécessaires afin de protéger certaines données contenues dans son système d'information, se traduisant, en cas de défaillance, par la mise en jeu de sa responsabilité civile et/ou pénale.

L'obligation de sécurité des données s'applique, notamment, au travers de l'article 34 de la loi Informatique et Libertés et de l'article 32 du règlement général sur la protection des données [15] (RGPD).

---

11. Condamnation pour accès et maintien frauduleux à un système de traitement automatisé de données, atteinte au secret des correspondances émises par voie électronique : TGI Annecy, 4 décembre 2015, Tefal et autres.
12. CA Paris, 4 octobre 2007, n° 06/02095, Association ARFP pour le téléchargement de fichiers contrefaits ; CA Paris, 29 octobre 2008, n° 06/14072, JurisData n° 2008-373540 ou CA Paris 10 avril 2014, n°11/04388, JurisData n°201-007648, consultation d'informations personnelles relatives aux dirigeants et collègues et téléchargement de musique, consultation de sites pornographiques.
13. Cass. Soc. 10 mai 2012, n° 11-11060 ; CA Metz, 24 février 2014, n°14/00120.
14. Cass. Soc., 17 juin 2009, n° 08.40274.
15. Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), applicable à partir du 25 mai 2018.

À ce titre, la CNIL se montre de plus en plus sévère en cas de défaut de sécurisation donnant lieu à une violation de données à caractère personnel [16]. Le code pénal sanctionne, d'ailleurs, le non-respect de ces dispositions [17].

D'autres réglementations, sectorielles le cas échéant, peuvent trouver à s'appliquer. À titre d'exemple, l'arrêté du 3 novembre 2014 [18] en matière bancaire, plus particulièrement ses articles 88 et suivants, oblige les banques à veiller « *au niveau de sécurité retenu et à ce que leurs systèmes d'information soient adaptés* » en prévoyant des audits réguliers, des procédures de secours ainsi que des mesures permettant de préserver en toutes circonstances l'intégrité et la confidentialité des informations ou encore le Code de la santé publique qui prescrit l'agrément des hébergeurs de données de santé ainsi que le respect de mesures de sécurité des systèmes d'information de nature à préserver le secret médical [19]. Le rôle de l'administrateur dépendra directement de l'environnement réglementaire dans lequel il exerce ses fonctions.

La jurisprudence a, en outre, tendance à attendre de l'entité qu'elle prenne la mesure de la nécessité de protéger son système d'information, sous peine de considérer qu'elle a contribué à son propre dommage [20].

La réglementation européenne est de plus en plus exigeante pour la sécurisation des données des entreprises et administrations en imposant, selon les cas, une obligation de notification des failles de sécurité et/ou de mise en place de mesures techniques et organisationnelles de gestion des risques menaçant la sécurité des réseaux et de l'information sous leur responsabilité [21]. Par ailleurs, le règlement général sur la protection des données, entrant en application en mai 2018, renforce les conséquences du défaut de sécurisation en augmentant le montant des sanctions pécuniaires pouvant être prononcées par la CNIL [22].

Attention

Par son action, l'administrateur contribue à assurer la sécurité du système d'information, obligation prescrite par de nombreux textes législatifs et réglementaires. Le non-respect de cette obligation peut engager la responsabilité civile et/ou pénale de l'entité.

À noter que l'administration sécurisée d'un système d'information passera également par la sécurisation des contrats dont l'entité est titulaire (contrats de travail, achat de matériel *software* ou *hardware*, prestations d'hébergement ou de sauvegarde, etc.). Des clauses essentielles à la bonne exécution des contrats sont à prévoir, telles que, notamment, les clauses de confidentialité, de sécurité, d'audit, de responsabilité incluant le cas échéant des pénalités, de continuité d'activité ou encore de réversibilité. Le risque est d'autant plus grand que le prestataire choisi peut être soumis, parfois, au respect de législations pouvant être considérées comme intrusives du point de vue de la sensibilité des données de l'entité.

---

16. Délibération de la formation restreinte n° 2014-298 du 7 août 2014 prononçant un avertissement à l'encontre de la société Orange : « *Si la société a remédié dans des délais satisfaisants aux faiblesses techniques relevées et a démontré pour l'avenir une meilleure prise en compte des problématiques de confidentialité des données, il n'en demeure pas moins qu'elle a manqué à son obligation d'assurer la sécurité et la confidentialité des données à caractère personnel de ses clients.* » ; Délibération de la formation restreinte n° 2015-379 du 5 novembre 2015 prononçant une sanction pécuniaire de 50 000 € à l'encontre de la société Optical Center pour défaut de sécurisation de sa base de données clients : « *la formation restreinte relève que le manquement relatif à la sécurisation du site était caractérisé au jour de l'expiration du délai de mise en conformité imparti et persistait au jour du second contrôle. Le fait que le protocole HTTPS est dorénavant en place sur l'ensemble du site est sans incidence sur la caractérisation de ce manquement.* »
17. Art. 226-17 du code pénal : cinq ans d'emprisonnement et 300 000 euros d'amende et art. 131-38 du code pénal : 1 500 000 euros pour les personnes morales ainsi que des peines complémentaires.
18. Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumis au contrôle de l'Autorité de contrôle prudentiel et de résolution.
19. Art. L. 1111-8 du Code de la santé publique.
20. CA Paris 4 mai 2007, Normaction c/ KBC Lease France, DMS, JurisData n° 2007-334142 ; TGI Paris, 21 février 2013, Sarenza c/ Jonathan et autres.
21. Directive (UE) n° 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Directive NIS).
22. Les sanctions prononcées par les autorités de contrôle pourront s'élever désormais jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires, le montant le plus élevé des deux étant retenu, règlement général sur la protection des données, art. 83. Précédemment, le montant maximal des sanctions pouvant être prononcées par la CNIL était de 150 000 euros.

L'assistance d'un conseil juridique spécialisé en la matière sera un atout lors de la négociation de celles-ci.

Attention

La sécurisation du système d'information doit être prévue aussi dans le cadre de clauses adaptées dans les contrats conclus par l'entité pour le fonctionnement de son système d'information. Ces clauses, selon le type de contrat concerné, peuvent pour partie avoir un impact sur l'étendue des pouvoirs de l'administrateur.

Enfin, la formation et la sensibilisation des collaborateurs à la nécessité de protéger le système d'information de l'entité ne doivent pas être négligées. En effet, certains comportement, pouvant pourtant donner lieu à sanctions (disciplinaires voire pénales), ne révèlent pas nécessairement d'intention de nuire mais uniquement une méconnaissance des conséquences potentiellement dommageables pour l'entité.

L'administrateur, en concertation avec le délégué à la protection des données le cas échéant, doit avoir une action essentielle en matière de sensibilisation. Celle-ci est une des mesures fonctionnelles à prévoir pour la sécurisation du système d'information.

Il reviendra à l'administrateur de surveiller l'utilisation des ressources du système d'information pour palier l'éventualité d'un incide.

Annexe C – Glossaire

À défaut de s'appuyer sur des définitions standardisées et dans un souci de clarté, le glossaire ci-dessous définit les termes spécifiques à ce guide :

Actions d'administration : ensemble des actions d'installation, de suppression, de modification et de consultation de la configuration d'un système participant au SI et susceptibles de modifier son fonctionnement ou d'altérer la sécurité du SI ;

Administrateur : un administrateur est une personne physique chargée des actions d'administration sur un SI, responsable d'un ou plusieurs domaines techniques ;

Administrateur métier, exploitant, intégrateur, support : l'administrateur métier ou le membre d'une équipe d'exploitation, d'intégration ou de support est considéré dans ce guide comme un sous-ensemble des administrateurs. C'est une personne physique en charge de l'exploitation ou de l'emploi d'un service ou d'une ressource d'administration en particulier.
Il dispose de privilège adapté à ces fonctions ;

Administration à distance : désigne tout accès au SI d'administration en dehors du réseau interne de l'entité ;

Authentifiant d'administration : combinaison d'un identifiant et d'un ou plusieurs secrets associés à un administrateur ou un service ;

Connexion à distance : depuis un poste de travail, la connexion à distance consiste à se connecter sur un autre environnement (physique ou virtuel) afin d'y ouvrir une session graphique (ex : RDP 24, ICA 25) ;

Compte d'administration :
Compte disposant de privilèges nécessaires aux actions d'administration, il peut être associé à un administrateur ou à un service logiciel ;

DMZ - *Demilitarized Zone* : une DMZ est une zone intermédiaire qui se situe entre deux réseaux ou systèmes d'information différents. Elle permet de protéger les ressources de la zone de plus haute sensibilité à l'aide d'un certain nombre d'outils de filtrage, voire de serveurs relais ;

Flux d'administration : flux de communication vers une ressource administrée pour la réalisation d'une action d'administration ;

Outils d'administration : outils techniques utilisés pour effectuer les actions d'administration (consoles, utilitaires, etc.) ;

Poste d'administration : terminal matériel, fixe ou portable, utilisé pour les actions d'administration ;

Réseau d'administration : réseau de communication faisant transiter les flux internes au SI d'administration et les flux d'administration à destination des ressources administrées ;

Ressources administrées : ce sont l'ensemble des dispositifs physiques ou virtuels du SI administré qui nécessitent des actions d'administration ;

Ressources d'administration : ce sont l'ensemble des dispositifs physiques ou virtuels du SI d'administration : poste d'administration, serveurs d'infrastructures d'administration, serveurs outils d'administration, etc. ;

SI d'administration : système d'information utilisé pour administrer des ressources qui sont présentes dans un autre SI dit SI administré, distinct du SI d'administration ;

Zone d'administration : sous-ensemble du SI d'administration dont l'objectif est d'isoler ou cloisonner des ressources d'administration par des mesures de protection adaptées au contexte (ex : filtrage, cloisonnement logique de réseau, authentification, mise en œuvre de VPN IPsec) et en fonction du juste besoin opérationnel. De façon à définir ces zones le plus efficacement possible, il est nécessaire au préalable de définir les zones de confiances du SI administré ;

Zone de confiance : ensemble de ressources informatiques regroupées en fonction de l'homogénéité de facteurs divers et variés (liés ou non à la sécurité).

DOCUMENT 10

« La mise en œuvre du RGPD dédramatisée au Congrès des maires ».

Gabriel ZIGNANI - Lagazettedescommunes.fr - Novembre 2018.

La mise en œuvre du Règlement général sur la protection des données personnelles (RGPD), qui inquiète de très nombreux maires, était au centre d'une table ronde au congrès des maires ce 21 novembre 2018. Une table ronde qui montre que c'est possible.

« En décembre 2017, aucune ligne n'était prévue au budget pour la mise en œuvre du RGPD. Nous n'en avions pas encore entendu parler. Le sujet est arrivé sur la table progressivement début 2018 ». Ces quelques mots de Jean-Claude Husson, maire de Saint-Arnoult-en-Yvelines (78), montrent l'une des raisons du retard qu'ont pris les collectivités dans la mise en œuvre des nouveaux textes qui réglementent la protection des données personnelles.

Mais dans cette commune, le retard a été en partie rattrapé. Car pour ce maire, « il y a de nombreux risques pour la collectivité. D'abord en termes d'images, mais il y a aussi des risques judiciaires, administratifs voire disciplinaires. » Mais la peur des sanctions n'est pas la seule raison qui a poussé Jean-Claude Husson a déclenché la mise en œuvre du RGPD. « Il ne faut pas oublier que si c'est une contrainte pour les collectivités, c'est aussi une protection pour les citoyens ». Pour ce faire, la première mesure qui a été prise dans sa commune, c'est la nomination d'un délégué à la protection des données (DPD), externalisé grâce au CIG 78.

Ce qui tombe bien, car Albine Vincent, cheffe du service des DPD à la Cnil, l'a rappelé : la priorité pour une collectivité territoriale, c'est de nommer un DPD, que ce soit en interne, ou qu'il soit mutualisé voire externalisé, « dont le rôle est d'informer, de conseiller et de contrôler.

Au-delà de son rôle, le délégué est important car il fait l'interface entre la collectivité et la Cnil, les agents, voire les habitants ».

Moins de temps que prévu

Armelle Guichard, juriste de la ville de Sceaux, a justement été nommé DPD de sa collectivité. Elles l'avouent : « les débuts étaient anxiogènes. Mais les choses se sont ensuite mises en place progressivement. » Tant et si bien que cette nouvelle fonction, qui s'ajoute à celle de juriste, lui a pris moins de temps que prévu.

Pour ce faire, elle s'y est prise en amont ! « J'ai commencé par sensibiliser les agents de la ville dès février dernier. Mon objectif était de les rassurer, de leur dire que le RGPD ne révolutionnerait pas leur manière de travailler. »

Elle a ensuite consacré « une quinzaine de jours » à la cartographie et l'établissement du registre : « J'ai auditionné les services un par un, afin d'établir la cartographie des traitements de données de l'ensemble de la municipalité. Cela m'a permis de faire un premier point sur la qualité de nos traitements, notamment sur leur proportionnalité et sur la durée de conservation des données.

J’en ai profité pour faire un premier ménage. » Il s’agit bien là d’une des grandes priorités indiquée par la Cnil dans la mise en œuvre du RGPD. Albine Vincent est revenue dessus devant les maires : « Il faut initier un travail de recensement des traitements mis en œuvre par la collectivité au plus vite, en se posant les questions : « quels sont les traitements que nous détenons ? » « Quelles données contiennent-ils ? » « Qui y a accès ? » … »

Retour sur les droits des personnes

Autre point de travail : la mise à jour de certains documents. « J’ai travaillé avec les différents services pour mettre à jour nos formulaires, en revoyant nos mentions de consentement. J’ai également mis à jour nos contrats avec nos prestataires. »

Armelle Guichard est aussi revenue sur les droits des personnes. La représentante de la Cnil avait auparavant ré insisté sur ce point : « Les collectivités doivent s’assurer de l’effectivité des droits des personnes, que ce soit le droit à l’information, de rectification …

Et ce même si la personne demandeuse est simplement curieuse et souhaite simplement savoir quelles données la collectivité détient sur elle. Elle y a droit. » Mais la déléguée de la commune de Sceaux n’a pas été beaucoup sollicitée dans ce cadre. « J’avais peur qu’avec la médiatisation qui a accompagné l’entrée en vigueur du RGPD, de nombreuses demandes arrivent, mais j’ai eu une seule requête. »